REMARKS

The pending claims stand rejected over Roese (20030217122) – singly or in combination with other art.

If the rejections are maintained, a Notice of Appeal will follow, together with a Request for Pre-Appeal Review.

One of the issues before the review panel and the BPAI will be the meaning of the claim term "*watermark* in the content" (or "*digital watermark* in the content").

In support of the Final Rejection, the Office notes, "*...applicant states a watermark being a transparent identifier inside a block of data...*"[1]

Applicant did not so state. (Nor is the Office's intended meaning of a "transparent identifier" clear.)

The review panel (and Board) will construe "watermark" and "content" in accordance with well-established rules of claim construction. As properly construed, they will agree that Roese does not teach the claimed arrangements.

Roese's system effects location-based access control through information conveyed in *header data*. Header data is different than "watermark data in the content."

To review, a packet consists of two types of data: header data and user data (also known as payload). "Watermark data in the content" is conveyed in the *user data* part of the packet (embedded in the content); not in the *header data*.

Header data (generally found at the beginning of a packet) typically provides information *about* a packet and its payload. For example, in standard IP packets, header data conveys the packet's source and destination addresses (32 bits each), the length of the packet (16 bits), a packet ID (16 bits), error detection/correction data (16 bits), and information specifically relating to the payload.

---

[1] Final Rejection, page 2, lines 13-14

If the payload is video, the header data specifically relating to the payload may include the bit-rate of the video, MPEG format type, content advisory data (V-chip), copy control information, and other tag (or flag) data.

The location restriction data taught by Roese is conveyed in header data (*see, e.g.,* paragraph [0116]). The Office maps this location restriction data to the "flag bits" language of claim 1

The Board will recognize, however, that these flag bits are *not* related to any "payload of a watermark in the content," as required by claim 1.

The Office argues that the usage identifiers "*would be transparent to the user as the user would not be aware of them or be able to modify them directly and must independently create any of the users desired usage rules. Therefore, Roese does teach the user of a tag placed in a header where the tag is determined by a transparent identifier inside the block of data.*"[2] The Office thus argues that the "watermark" limitation is met.

This won't pass appellate review. *None* of the information in the header is visible to users. The user is not "aware" of packet address bits, error correction bits, or any of the other header data. "Transparent" to the user does not a watermark make.

The logic advanced in the Final Rejection would argue that *all* of the header data is watermark data. In fact, none of it is.

The claim requires that the (header) flag bits "*be related to the payload of a watermark in the content*." Roese does not teach any arrangement in which header data is related to information watermarked in the content (i.e., non-header data).

[2] Final Rejection, text bridging pp. 2-3.

Moreover, there is no watermark teaching in Roese. The Wikipedia entry for digital watermarking currently states:

> In invisible watermarking, information is added as digital data to audio, picture or video, but it cannot be perceived as such. An important application of invisible watermarking is to copyright protection systems, which are intended to prevent or deter unauthorized copying of digital media. Steganography is an application of digital watermarking, where two parties communicate a secret message embedded in the digital signal. Annotation of digital photographs with descriptive information is another application of invisible watermarking. While some file formats for digital media can contain additional information called metadata, digital watermarking is distinct in that the data is carried in the signal itself.[3]

A simple example of digital watermarking applied to audio or video is to change the least significant bit of each audio or image data sample so that the LSBs repesents the bits of the watermark message.

There is no "watermark in the content" taught by Roese.

The Office is invited to correct these clear errors in the Final Rejection of claim 1 before the case is appealed.

(Attached to the end of these remarks is a possible amendment to claim 1 that could be made if it would help put the claim in condition for allowance. However, as detailed above, the pending claim is properly allowable as-is.)

[3] Applicant does not wholly adopt the Wikipedia understanding. For example, many researchers regard digital watermarking as a subset of steganography, rather than vice versa. However, applicant's understanding does not control; the Board's interpretation is the relevant one.

Regarding claim 4, the Office is requested to more particularly identify the counterpart to the claimed "additional data" in Roese. Applicant finds no data in Roese that meets the claim requirements.

Roese certainly teaches a system that limits distribution of protected information beyond certain boundaries. But that broad concept, *per se,* is not being claimed.

Rather, claim 4 concerns a method of forming header data in an IP packet, where the data includes "additional data" having two states respectively indicating certain restrictions. Roese does not teach the particularly-detailed method.

Claim 11 has been rejected with the statement "*the claim is rejected for the same reasons as claim 4 above*." However, it will be recognized that claim 11 has limitations not found in claim 4, e.g., concerning physical location and proximity. Moreover, claim 11 includes limitations about the destination address specified in the packet header data. None of these limitations has a counterpart in claim 4.

More striking is the rejection of claim 19. Again the claim is rejected "*for the same reasons as claim 4 above,*" but the claims don't even have a superficial similarity.

Claim 19 requires obtaining an identifier of the content, and including same in the "second portion" of each packet. No such teaching is found in Roese.

The foregoing has just touched on some of the problems with the rejections of certain independent claims. However, such remarks are believed to establish that none of the rejections would be sustained on review. The Office is invited to address the noted deficiencies before such review.

Notwithstanding strenuous disagreements with the present rejections – a few of which are noted above, and others of which will be detailed in the appeal – applicant would be pleased to consider canceling certain claims from the present application and continuing them in a new application, if common ground could be found regarding allowability of some of the other claims. The Examiner is invited to telephone the undersigned if he sees potential for such common ground.

Respectfully submitted,

Date: June 13, 2008

DIGIMARC CORPORATION

CUSTOMER NUMBER 23735

Phone: 503-469-4800
FAX 503-469-4777

By /William Y. Conwell/
William Y. Conwell
Registration No. 31,943

Possible Amendment to Claim 1

1. A method of enforcing geographical restrictions on content redistribution in a TCP/IP network **in which content is distributed in packet form, each packet including header data and content data, the header data comprising information about the packet and its payload, the method comprising the acts** ~~, comprising~~:

defining a geographical boundary across which certain content **data** does not pass, wherein said boundary is defined – at least in part – by a hardware firewall device; and

determining whether an IP packet should be regarded as conveying content that should not cross said boundary, by reference to one or more flag bits included in the header **data** of said packet;

wherein said one or more flag bits are related to the payload of a watermark in the content **data**.